IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants:	Neal A. KRAWETZ	Confirmation No.: 9182
Application Serial No.:	09/975,815	
Filed:	October 11, 2001	
Title:	SYSTEM AND METHOD FOR SECURE DATA TRANSMISSION	
Group Art Unit:	2436	
Examiner:	Colin, Carl	
Docket No.:	10019968-1	

MAIL STOP: APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

REPLY BRIEF

Appellant respectfully submits this Reply Brief in response to the Examiner's Answer mailed January 8, 2009, pursuant to 37 C.F.R. §41.41.

STATUS OF CLAIMS

Claims 1-34 stand rejected pursuant to a final Office Action mailed June 12, 2008 ("Office Action"). Claims 1-34 are presented for appeal.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-34 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

2. Claims 1-2, 4-5, 7-8, 11-12, 14, 15, 19 and 22-25 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,931,128 to Roberts (hereinafter "*Roberts*").

3. Claims 3, 6, 9, 10, 13, 16-18, 20, 21 and 26-34 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Roberts* in view of U.S. Patent No. 6,751,736 to Bowman, et al. (hereinafter "*Bowman*").

ARGUMENT

In response to the Examiner's Answer, the Appellant provides the following rebuttal.

1. *Rejection under 35 U.S.C. §112*

The Appellant observes that MPEP §2163.02 states:

> The courts have described the essential question to be addressed in a description requirement issue in a variety of ways. An objective standard for determining compliance with the written description requirement is, "does the description clearly allow persons of ordinary skill in the art to recognize that he or she invented what is claimed." *In re Gosteli*, 872 F.2d 1008, 1012, 10 USPQ2d 1614, 1618 (Fed. Cir. 1989). Under *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563-64, 19 USPQ2d 1111, 1117 (Fed. Cir. 1991), to satisfy the written description requirement, an applicant must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention, and that the invention, in that context, is whatever is now claimed.

(emphasis added)

Keeping the above standard dictated by the MPEP in mind, Appellant notes that the Appellee states on page 23 of the Examiner's Answer:

> The fact that the encryption key changes with each transmitted data packet does not inherently or implicitly mean a character string is generated for each data packet associated with the secure data transmission because a change in the encryption key even when assuming it is the hash key can be caused by any one of the two sets of data or by none of them (i.e. other means by adding salt to the encryption key.)

(emphasis added).

Thus, in the above-quoted portion of the Examiner's Answer, the Appellee appears to suggest that there are different methods for generating a unique encryption key for each data packet where a character string and a private key are involved. However, the Appellee in doing so, appears to look beyond Appellant's disclosure. Appellant's disclosure clearly discloses a method for generating a unique encryption key for each data packet where a character string and a private key are

involved. See, for example, page 8, lines 25-27, page 4, lines 20-22, and block 210 of Fig. 2. Therefore, the Appellee appears to be reaching outside the Appellant's disclosure in an effort to support the rejection under 35 U.S.C. §112. The Appellant submits that looking beyond the Appellant's disclosure in the manner that the Appellee has done in an attempt to justify the rejection under 35 U.S.C. §112 is improper. For this reason alone, the Appellee's rejection under 35 U.S.C. §112 should be reversed by the Board.

Further, the Appellant submits that, despite the Appellee's indication to the contrary, there was an express disclosure in the Application as originally filed supporting the amendments made to the claims. Indeed, on page 8, in lines 25-27, of the originally-filed disclosure, Appellant expressly states that "unlike secure shell or other tunneling protocols, the encryption key changes with each transmitted data packet" (emphasis added). As disclosed on page 4, lines 20-22, and illustrated in block 210 of Fig. 2, the encryption key (a.k.a., the hash key 64) is generated using the character string 54 and the private key 62. Appellant submits that one skilled in the art would recognize that the variable used to generate the hash key 64, namely the character string 54, is changed to generate a hash key 64 that "changes with each transmitted data packet" as expressly disclosed on page 8, in lines 25-27, of the originally-filed disclosure. For example, at least on page 4 of the originally-filed disclosure, it is stated that "the string generator randomly generates and stores the character string," and that the character string is hashed with the private key to generate the hash key (page 4, lines 19-33).

For each of the foregoing reasons, Appellant submits that Appellee's rejection of Claim 1 does not appear to be well founded. Therefore, Appellant respectfully requests that the Board reverse Appellee's § 112, 1st paragraph, rejection of Claim 1.

At least for the reasons discussed above in connection with independent Claim 1, Appellant respectfully submits that the amendments to Claims 11, 19 and 27 in the Response are also supported by the originally-filed specification. As such, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 11, 19 and 27.

Each of Claims 2-10, 12-18, 20-26 and 28-34, either directly or through intervening claims, depends from and includes all the base limitations of independent Claims 1, 11, 19 and 27, respectively. As such, each of Claims 2-10, 12-18, 20-26

and 28-34 is believed to comply with the written description requirement of § 112, 1st paragraph, for at least the reasons noted above for Claims 1, 11, 19 and 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 2-10, 12-18, 20-26 and 28-34.

2. *Rejection under 35 U.S.C. §102(e) over Roberts*

a. *Claims 1-2, 4 and 8*

In support of the rejection of Claims 1-2, 4 and 8 under 35 U.S.C. §102(e), the Appellee states on page 26 of the Examiner's Answer:

> Roberts clearly discloses, see column 6, lines 45-54, both the first and second computer systems negotiate a master secret key that is to be known by only (unique to) the first and second computer systems and a security parameter index associated with the master secret is also negotiated. Therefore, the SPI is associated with the sender or first computer system.

(emphasis in original).

The Appellant respectfully disagrees. As noted in MPEP § 2141.02 VI., a prior art reference must be considered in its entirety, i.e., as a whole. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). Against this backdrop, the Appellant submits that the most reasonable interpretation of *Roberts* does not appear to be the interpretation made by the Appellee.

Roberts states in Col. 6, lines 45-54:

> As illustrated by FIG. 4, before secure communications begin, the first and second computer system securely negotiate a master secret (act 401) that is to be known by only the first and second computer systems. Other parameters such as a Security Parameter Index (SPI), a parameter expiry, and an algorithm suite may also be negotiated in the same session[.] Technology for securely negotiating a master secure [sic] are [sic] well known in the art and may include using asymmetric encryption technology.

(emphasis added).

Roberts also states in Col. Col. 9, line 65 - Col. 10, line 7:

> A Secure Parameter Index (SPI) is a 96 bit (12 byte) bit sequence that is unique to the second computer system. The SPI may be included to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol ... The data packet 204 is then transmitted to the second computer system (act 409) for decryption by the decryption device 202.

(emphasis added).

Roberts further states in Claim 21:

> [A] method of the second computer system ..., the method comprising the following:
>
> an act of securely negotiating a master secret with the first computer system;
>
> an act of receiving plurality of encrypted data packets from the flint [sic] computer system, wherein the first computer system encrypts every data packet with a different key based on a different random seed, such that each encrypted data packet received by the second computer system is encrypted with a different key based[.]

(emphasis added).

Based on the above, Appellant respectfully submits that the Secure Parameter Index (SPI) is unique to the second computer system. Therefore, when *Roberts* is taken as a whole, Appellant submits that the SPI is associated solely with the receiving computer system. Thus, the second or receiving computer in *Roberts* may receive encrypted data packets from any of a number of different computers and decryption of the data packets by the second computer is not based or contingent upon the identity of the sender. In contrast, Claim 1 recites that the sender "transmit[s] an identification key associated with the sender" (emphasis added). The SPI of *Roberts* is not associated with the sending computer system and, in fact, appears to be used by any sending computing system. Therefore, the SPI of *Roberts* is not associated with the sending computer system, nor does the SPI of *Roberts* identify the sending computer system in any way.

Moreover, as stated in MPEP § 2111, during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). However, the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999). Here, it is respectfully submitted that the Appellee is interpreting the claim limitation "associated" in a manner that is repugnant to the common understanding of that term in order to reject the claims with *Roberts*. The Appellant submits that the "negotiation" involving the SPI taking place between the first and second computer systems in *Roberts* has nothing at all to do with, nor does it teach or suggest, that the SPI is "associated" with the first computer system or in any way identifies the first computer system.

In addition to the above, in support of the rejection under 35 U.S.C. §102(e) the Appellee generally states on page 26 of Examiner's Answer for the first time during prosecution that the "identifying label" of *Roberts* meets the claim limitation of an identification key associated with the sender, that the "label" being concatenated with the random seed and transmitted to the second computer system meets the claim limitation of transmitting an identification key associated with the sender, and that disclosing "the first and second computer negotiating a parameter expiry identifying the valid lifetime of the master secret" meets the claim limitation of an identification key associated with the sender. Appellant respectfully submits that in each instance, the alleged "key" identified by the Appellee is simply not associated with the sender as claimed and that the above-referenced purported disclosure of *Roberts* in no way identifies the sender to the receiving computer.

Based upon the above, the Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 1. Also, each of Claims 2, 4 and 8, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 1. As such, each of Claims 2, 4 and 8 is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 2, 4 and 8.

b. *Claims 5 and 7*

In support of the rejection of Claims 5 and 7 under 35 U.S.C. §102(e), the Appellee states on page 27 of Examiner's Answer:

> [A]n identification key is implicitly used to identify a key and the SPI is by definition an identification tag added to the header of the data packer to determine which encryption algorithms and rules to use[.]

(emphasis added).

Appellant respectfully disagrees with the Examiner's assertions. Each of Claims 5 and 7 recites, *inter alia*, "determining the private key at the recipient using the identification key." On page 27 of the Examiner's Answer, the Appellee appears to equate the "identification key" as recited in the claims to the Secure Parameter Index (SPI) of *Roberts* and now asserts that *Roberts* discloses the above-quoted limitation in Col. 6, lines 45-54, Col. 7, lines 2-5 and 45-55, Col. 9, lines 45-52 and 62-63, and Col. 13, lines 6-30.

In Col. 6, lines 45-54, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) is unique to the second computer. In addition, in Col. 7, lines 2-5, *Roberts* only appears to indicate that lower overhead symmetric encryption algorithms may be used in which the same key that is used to encrypt data is used to decrypt data. In Col. 9, lines 45-52 and 62-63 and Col. 13, lines 6-30, *Roberts* only appears to indicate that the Secure Parameter Index (SPI) may be included in the data packet to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol. Therefore, Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is used in "determining the private key at the recipient using the identification key" as recited in Claims 5 and 7.

Moreover, in contrast to the definition that the Appellee attempts to assign to the Secure Parameter Index (SPI), the Appellant notes that *Roberts* expressly defines the SPI in Col. 9, lines 65-67, through Col. 10, lines 1-2, as:

> A Secure Parameter Index (SPI) is a 96 bit (12 byte) bit sequence that is unique to the second computer system. The SPI may be included to ensure compatibility with the Encapsulation Security Payload (ESP) protocol of the Internet Protocol Security (IPSec) protocol.

(emphasis added).

Based on the above, the Appellant submits that *Roberts*, acting as his own lexicographer as authorized by MPEP § 2111.01, gave the term "Secure Parameter Index (SPI)" a specific definition in light of, for example, Claim 22 in *Roberts*. Therefore, in contrast to the definition of the SPI advocated by the Appellee, Appellant submits that *Roberts* clearly and expressly defines the SPI as a sequence used to ensure compatibility. Therefore, the Appellee has not pointed out, and the Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is used in "determining the private key at the recipient using the identification key" as recited in Claims 5 and 7. As such, *Roberts* does not appear to anticipate Claims 5 and 7.

Based on the foregoing, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 5 and 7. Also, each of Claims 5 and 7, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 1. As such, each of Claims 5 and 7 is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 5 and 7.

c. *Claims 11, 12, 14-15, 19 and 22-24*

In support of the rejection of Claims 11, 12, 14-15, 19 and 22-24 under 35 U.S.C. §102(e), the Appellee states on page 28 of Examiner's Answer that the rejection of these claims should be sustained for the reasons set forth by the Appellee in regard to Claims 1, 5 and 7. In similar fashion, the Appellant submits that the rejection of independent Claims 11 and 19, and those claims depending therefrom, should be reversed for the reasons noted above for Claims 1, 5 and 7.

d. *Claim 25*

In support of the rejection of Claim 25 under 35 U.S.C. §102(e), the Appellee repeats on page 28 of Examiner's Answer, almost *verbatim*, the same rationale purportedly supporting the rejection of Claims 5 and 7. The Appellant notes that the scope of Claim 25 and the scope of Claims 5 and 7 is quite different.

Claim 25 recites, *inter alia*, "the recipient is adapted to determine the hash key using the identification key and the character string" (emphasis added). In contrast, each of Claims 5 and 7 recites, *inter alia*, "determining the private key at the recipient using the identification key" (emphasis added). Despite the dissimilarity in scope between Claim 25 and Claims 5 and 7, the Appellee nonetheless attempts to support the rejection of all of the claims with the same rationale. Because Claim 25 has a different claim scope as compared to Claims 5 and 7, which the Appellee does not appear to have appreciated, the Appellant submits that the rejection of Claim 25 is not well founded. As an example, the Appellee states on page 28 that:

> [T]he SPI is by definition an identification tag[.] … Thus, at the recipient side, the master secret is determined using the identification tag (SPI). In addition, Roberts discloses an identifying label for generating a key at the sender (see column 7, lines 45-55), the label is concatenated with the random seed and transmitted to the second computer system (see column 9. lines 45-52 and 62-63). Thus, the random seed, which includes the identifying label is used to generate a hash key (see column 7, lines 45-55).

Based on the above, the Appellee appears to acknowledge that the random seed and the identifying label, and not the identification tag (SPI), are used to generate the hash key. As such, the Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 25.

In addition, Claim 25 depends from and includes all the base limitations of independent Claim 19. As such, Claim 25 is believed to be patentable for at least the reasons noted above for Claim 19. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 25.

3. *Rejection under 35 U.S.C. §103(a) over Roberts in view of Bowman*

a. *Claims 27 and 28-34*

In support of the rejection of Claim 27 under 35 U.S.C. §103, the Appellee quotes and reproduces on pages 29-30 of the Examiner's Answer several portions of both *Roberts* and *Bowman*. However, Appellant submits that those portions of *Roberts* and *Bowman* do not appear to teach or suggest an "identification key," much less an identification key that identifies a particular client. Indeed, the Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Roberts* that the Secure Parameter Index (SPI) is employed as "an identification key" as recited in Claim 27, much less an identification key identifying a particular client as defined by the originally-filed Application. In addition, the Appellee has not pointed out, and Appellant is unable to locate, any teaching or suggestion in *Bowman* that the Secret ID is employed as "an identification key" as recited in Claim 27, much less an identification key identifying a particular client as defined by the originally-filed Application.

In addition, in response to the Appellant pointing out in the Appeal Brief that the identification key may comprise a serial number or other type of identifier indicating the particular client 18 transmitting the data, on page 30 of the Examiner's Answer the Appellee states:

> Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims.

Appellant submits that the argument presented in Appellant's Appeal Brief is to make more clear the differences between the recited "identification key" and the SPI of *Roberts* such that the SPI of *Roberts* performs no "identification" function.

Further, in response to the Appellant's assertion that *Roberts* and *Bowman* would not be combined by one skilled in the art, the Appellee states on page 31 of the Examiner's Answer that *Roberts* indicates the SPI is included in the data packet. However, as clearly noted in Col. 6, lines 45-49, of *Roberts*:

> As illustrated by FIG. 4, before secure communications begin, the first and second computer system securely negotiate a master secret (act 401) that is to be known by only the first and second computer systems.

(emphasis added).

When the above is read in context with the remainder of *Roberts*, especially those paragraphs immediately following the above-quoted paragraph, *Roberts* appears to disclose that the data packets transmitted during secure communications are not sent or received until after the master secret has been negotiated. Thus, as originally advocated in the Appellant's Appeal Brief, *Roberts* and *Bowman* would not be combined by one skilled in the art.

Based on the foregoing, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 27. Also, each of Claims 28-34, either directly or through intervening claims, depends from and includes all the base limitations of independent Claim 27. As such, these claims are believed to be patentable for at least the reasons noted above for Claim 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 28-34.

b. *Claims 3, 10 and 20*

In support of the rejection of Claims 3, 10 and 20 under 35 U.S.C. §103(e), on pages 31-32 of the Examiner's Answer the Appellee acknowledges a typographical error and then states:

> Examiner asserts that there is enough teaching and suggestion of the prior art in addition to the knowledge of one of ordinary skill in the art to recognize the advantage to use the hash key instead of the private key to generate the signature for better security[.]

Appellant respectfully disagrees. Referring to Fig. 6 of *Bowman*, if *Bowman* is modified as suggested (and interpreted) by the Appellee, then the "hash key" 640, and not the "secret string (private key)" 631, is used to generate the "signature" 624. However, Appellant submits that such a modification of *Bowman* results in the "signature" 624 being formed from the "data" 615, the "secret string (private key)" 631, and the "SALT" 670 and the "hash key" 640 being formed from the "secret string (private key)" 631 and the "SALT" 670. As a result, it appears to the Appellant that the only input not common to both the "signature" 624 and the "hash key" 640 of *Bowman* as modified by the Appellee is the "data" 615. Thus, if the "signature" 624

and the "hash key" 640 were compromised and the common inputs (i.e., the "secret string (private key)" 631 and the "SALT" 670) identified or isolated, only the "data" 615 would remain, thereby leaving the "data" 615 vulnerable in this manner appears to be counterintuitive in the art of cryptology.

In addition to the above, modifying the "signature" 624 of *Bowman* such that the "signature" 624 and the "hash key" 640 share further common inputs appears to diminish the independence of the "signature" 624 and the "hash key" 640 relative to one another. Therefore, the Appellant suggests that one skilled in the art would not modify *Bowman* in the manner suggested by the Appellee.

Also, Claims 3, 10 and 20, either directly or through intervening claims, depend from and includes all the base limitations of independent Claims 1 and 19, respectively. As such, these claims are believed to be patentable for at least the reasons noted above for Claims 1 and 19. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 3, 10 and 20.

c. *Claim 9*

In support of the rejection of Claim 9 under 35 U.S.C. §103(e), on pages 33-34 of the Examiner's Answer the Appellee asserts that Claims 3 and 4 of *Bowman* disclose a "first signature" and a "second signature." Appellant respectfully disagrees and submits that any purported first and second signature of *Bowman* does not teach or suggest the "first signature" and "second signature" as recited in Claim 9.

Claim 9 recites, *inter alia*, "generating a first signature by the sender using the hash key and the data. In contrast, Claim 3 of *Bowman* appears to disclose that the "first signature" is produced by hashing the plurality of descriptors concatenated with the secret string (i.e., descriptor-secret string). Because the "first signature" of *Bowman* is produced with the secret string instead of a hash key, the Appellant submits that the "first signature" of *Bowman* does not appear to be a first signature as recited in Claim 9.

In addition, Claim 9 recites, *inter alia*, "compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data." In contrast, Claim 4 of *Bowman* appears to disclose that the "second signature" is produced by hashing the plurality of descriptors concatenated with the secret string. Because the second signature of *Bowman* is produced with the secret string and the

plurality of descriptors instead of a hash key and decrypted data, the Appellant submits that the "second signature" of *Bowman* does not appear to be a second signature as recited in Claim 9.

Based on the foregoing, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 9. In addition, Claim 9 depends from and includes all the base limitations of independent Claim 1 and is believed to be patentable for at least the reasons noted above for Claim 1. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claim 9.

d. *Claims 6, 13, 16-18, 21, 26 and 28*

Claims 6, 13, 16-18, 21, 26 and 28 depend from and include all the base limitations of independent Claims 1, 11, 19 and 27, respectively. As such, these claims are believed to be patentable for at least the reasons noted above for Claims 1, 11, 19 and 27. Therefore, Appellant respectfully requests that the Board reverse Appellee's rejection of Claims 6, 13, 16-18, 21, 26 and 28.

CONCLUSION

Appellant has demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Appellant respectfully requests the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

No fee is believed due with this Reply Brief. If, however, Appellant has overlooked the need for any fee, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

/James L. Baudino/
James L. Baudino
Reg. No. 43,486

Date: March 2, 2009

Hewlett-Packard Company
Intellectual Property Administration
18110 S.E. 34th St.
Vancouver, WA 98683